

What is claimed is:

1. A code computing apparatus comprising:

first and second registers (201 and 202) in which  
parameters having a predetermined bit length are set,  
5 respectively;

a third register (203) in which data to be encrypted is  
set;

a matrix element computation part (30) for generating  
matrix elements from the values set in said first and second  
10 registers;

a matrix element register (51) for holding the matrix  
elements generated by said matrix element computation part;  
and

an inner product calculation part (40) for executing inner  
15 product calculation between the matrix elements held by said  
matrix element register and the data set in said third register,  
wherein

said matrix element computation part selectively  
generates matrix elements for error detection and matrix  
20 elements for encryption by changing the parameters to be set  
in said first and second registers, and

said inner product calculation part selectively performs  
error control code generation and data encryption by altering  
the matrix elements to be held in said matrix element register.

2. A code computing apparatus comprising:

first and second registers (201 and 202) for storing,  
at least one of them, coefficient data of a polynomial of degree  
n;

5 a third register (203) in which data to be encrypted is  
set;

a matrix element computation part (30) for generating  
matrix elements of  $n \times n$  from the value set in said first and  
second registers;

10 a matrix element register (51) for holding the matrix  
elements generated by said matrix element computation part;  
and

an inner product calculation part (40) for executing inner  
product calculation between the matrix elements held by said  
15 matrix element register and the data set in said third register;  
wherein

said inner product calculation part produces encrypted  
data of transmitting data or receiving data supplied to said  
third register.

20

3. The code computing apparatus according to claim 2, wherein

said matrix element computation part generates matrix  
elements for error detection, and said inner product calculation  
part generates an error detection code corresponding to the  
25 data set in said third register.

4. The code computing apparatus according to claim 3, wherein  
coefficient data ( $g'$ ) of a polynomial  $g(x)$  of degree  $n$   
of Galois field is set, except for a coefficient of the highest  
5 degree  $n$ , to said first and second registers, and

said inner product calculation part outputs a CRC code  
corresponding to a modulus (mod) of the polynomial  $g(x)$  for  
the data set in said third register.

10 5. The code computing apparatus according to claim 2, wherein  
said matrix element computation part generates matrix  
elements for encryption, and

said inner product calculation part outputs an encryption  
code of the data set in said third register.

15

6. The code computing apparatus according to claim 5, further  
comprising:

a first memory for storing coefficient data of an  
irreducible polynomial  $g(x)$  of degree  $n$  of Galois field and  
20 encryption key data;

a control part (70) for reading out from said memory the  
coefficient data and the encryption key data in a form divided  
into a plurality of data blocks and setting them in said first  
and second registers, respectively, and

25

a second memory for storing elements values of a plurality

of partial matrices, wherein

elements of a plurality of partial of matrix of  $n \times n$  are generated by said matrix element computation part (30), and

under the control of said control part, the elements of  
 5 partial matrix generated by said matrix element computation part are stored in said second memory, the elements of partial matrix are selectively loaded from said second memory to said matrix element register (51), and said inner product calculation part repeats the inner product calculation between the data  
 10 set in said third register and the elements of a plurality of partial matrices, thereby to output said encryption code.

7. The code computing apparatus according to claim 6, further comprising:

15 means (52 and 53) for performing exclusive OR operation between the results of inner product calculation generated by said inner product calculation part and pre-computed elements held as intermediate results of the calculation, and holding the results of exclusive OR operation as new intermediate results  
 20 of the calculation.